ORIGINAL

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF TEXAS

FORT WORTH DIVISION

UNITED STATES OF AMERICA	§	
	§	
v.	§	**4-14-CR-023-A**
	§	
CHRISTOPHER ROBERT WEAST (1)	§	

MOTION TO SUPPRESS EVIDENCE SEIZED AS A RESULT OF AN UNLAWFUL SEARCH AND SEIZURE

Now comes Defendant CHRISTOPHER ROBERT WEAST, through undersigned counsel, and moves to suppress the following evidence as obtained in violation of his right to be free from unlawful searches and seizure, to due process of law, and to the effective assistance of counsel as guaranteed by the Fourth, Fifth, and Sixth Amendments to the United States Constitution:

1. All evidence and information, including, but not limited to, items seized by law enforcement officials during or a result of the search executed on or about July 10, 2012, of the residence at 833 Hallvale Drive, White Settlement, Tarrant County, Texas 76108 and any statements made by the defendant as the result of such search and seizure, and any fruits of such search.

Defendant further requests this Court to hold a pretrial evidentiary hearing to determine whether the above-described evidence should be suppressed.

I.

Introduction and Factual Background

Defendant is charged by third superseding indictment in Count One, with possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2); and in Count Two, with receipt of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(2); and Count Three, a forfeiture count.

On July 10, 2012, a search warrant application and supporting affidavit from Officer Randy D. Watkins, with the Crimes Against Children Unit of the Fort Worth Police Department, for the above referenced location, was presented to Fort Worth Municipal Judge Gonzales. The search warrant was issued and executed on that same date. As a result of the warrant's execution, the items of child pornography were allegedly found on the defendant's computer and on a Western Digital external hard drive located in what was determined to be the defendant's bedroom of the residence.

The affidavit in support of the search warrant states the following on the sixth page of the affidavit, starting with the second paragraph:

> On 6/4/12 at approximately 1420 hours, using a program called Child Protection System, the Affiant located an Internet Protocol (IP) address that was offering to participate in the Promotion of Child Pornography. The IP address was 99.71.201.174. The suspect IP address was offering to share files via the Internet on the Gnutella Network. Using the Child Protection System program, the Affiant could see under the "Unique Files" section that the suspect IP address had 3543 categorized files and that 1761 of those files were "Child Notable"(images and/or videos of known child pornography). The Child Protection System program compares the SHA values of the images and/or videos against a database of SHA files that law enforcement officers have looked at and believe to contain suspected or known child pornography. ** SHA is a Secure Hash Algorithm, similar to an electronic fingerprint for files. The chance of two files having the same SHA and different content is astronomical.
>
> Using an additional program called ShareazaLE, the Affiant attempted to download these "child notable" files from the suspect IP address. As ShareazaLE was downloading the files from IP 99.71.201.174, the Affiant noticed in the log files that the computer nickname being downloaded from was named "Chris".

> The downloaded images/videos were automatically stored in a download file under the IP address of 99.71.201.174. The first download took place on 6/4/12 at 14:21 local time. Adding 5 hours to the local time, this converts to 19:21 GMT. The following is a description of some of the photographs downloaded from the suspect IP:

The affidavit then proceeds to list the file names and descriptions of six photographs the officer believed to contain child pornography. Officer Watkins (the affiant) then states that 66 images of what he claims to be child pornography or suspected child pornography were downloaded from the suspect IP address. The affidavit states the following on page seven, starting on the third paragraph:

> The suspect IP address was checked using centralops.net and found to be owned by SBC Internet Services, Inc.
>
> On 6/6/12 using this information, the Affiant prepared a written subpoena request for account information on who was assigned IP address 99.71.201.174 on 6/4/12 at 19:21 GMT (1421 hours central time). The subpoena request was sent to the Tarrant County District Attorney's Office for processing.
>
> On 6/20/12, the Affiant received the subpoena return from SBC Internet Services with account information on who/what account was assigned Internet Protocol (IP) address 99.71.201.174 on Monday, June 4, 2012 at 19:21 GMT. The SBC Internet Services subpoena return showed that on this date and time that IP address was assigned to account #116103070, Larry Weast, telephone #817-246-3866, 833 Hallvale Drive, white Settlement, Texas 76108.

The defendant contends that the search in question is unconstitutional because the information contained in the search warrant affidavit was obtained as the result of warrantless and unlawful searches and seizures in violation of the Fourth Amendment to the United States Constitution. The basis of this argument is essentially two fold:

> 1) The pre-warrant search of the defendant's computers (using the Child Protection System and ShareazaLE computer programs) to determine what images were contained on the computers and to determine the Internet Protocol (IP) address for the computers were Fourth Amendment searches violating the defendant's reasonable expectation of privacy on his home computers; and

2) The use of a grand jury subpoena to obtain the subscriber information for the IP address from SBC Internet Services was also a warrantless search of information for which the defendant had a reasonable expectation of privacy under the Fourth Amendment

II.
Authority

FOURTH AMENDMENT

The Fourth Amendment to the United States Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Where a Fourth Amendment violation has occurred, the exclusionary rule mandates the suppression of not only all evidence obtained in the illegal search or seizure itself; it also requires the suppression of all evidence obtained as a result of, or derivatively from, the illegally seized evidence, as such derivative evidence is the "fruit of the poisonous tree." *Wong Sun v. United States,* 371 U.S. 471, 488 (1963).

Where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, . . . reasonableness generally requires the obtaining of a judicial warrant." *Riley v. California* ___ U.S. ___, 134 S. Ct. 2473, 2482 (2014). In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement. *Id.*

III.
Argument

In this particular case, the affidavit in support of the search warrant relies on two critical categories of information to establish probable cause, both of which were obtained without a warrant. Again, those two categories of information are: 1) the images that were found on a computer and the

IP address of that computer – these items having been discovered by law enforcement using the programs "Child Protection System" and "ShareazaLE" to search the defendant's computer; and 2) the subscriber information connected to this IP address through use of a grand jury subpoena. The defendant had a Fourth Amendment expectation of privacy in both his computer and the information related to its IP address in the possession of the internet provider.

The defense recognizes the above arguments have essentially been rejected by other Courts of Appeals outside of the Fifth Circuit. Specifically, several courts have found that there is no expectation of privacy in publicly shared, peer-to-peer files, or the IP addresses for the computers. *See United States v. Borowy*, 595 F. 3d 1045, 1048 (9th Cir. 2010); *United States v. Christie*, 624 F.3d 558, 574 (3rd Cir 2010); *United States v. Stultz*, 575 F.3d 834, 842-45 (8th Cir. 2009); *United States v. Perrine*, 518 F.3d 1196, 1205 (10th Cir. 2008).

Also, other courts have found that there is no legitimate expectation of privacy in the subscriber information connected to such IP addresses. *See United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010); *Perrine*, 518 F.3d at 1204.

One district Court case out of the Western District of Texas does reject this defendant's argument, in a decision that provides a thorough analysis of the argument. *United States v. Dodson*, 960 F. Supp. 2d 689 (W.D. Texas, Aug. 13, 2013).

Nevertheless, the defense has been unable to find any Fifth Circuit opinion or Supreme Court opinion that specifically rejects this argument that the defendant has an expectation of privacy for the information contained on his computer, his IP address for that computer, and the subscriber information connected with that IP address. Accordingly, the defendant is raising this issue for this Court's determination as an issue of first impression in this Circuit as well as to preserve the issue

for further review, particularly in light of the recent Supreme Court decision in " *Riley v. California*, 134 S. Ct. 2473 (2014) (holding that defendants do have an expectation of privacy with regard to their cell phones).

Wherefore, the defendant prays that the search of the residence in question should be suppressed along with all the fruits of the search, including any items seized as a result of the search and any statements made by the defendant resulting from the search.

Respectfully submitted,

JASON HAWKINS
Federal Public Defender
Northern District of Texas

BY: _____
Angela Saad
Asst. Federal Public Defender
819 Taylor Street, Room 9A10
Fort Worth, TX 76102-4612
(817) 978-2753
Texas State Bar No. 24059016

CERTIFICATE OF CONFERENCE

I have conferred with the attorney for the government, Aisha Saleem, and she is opposed to this motion.

_____
Angela Saad

CERTIFICATE OF SERVICE

I, Angela Saad, hereby certify that on July 18, 2014, the above motion was had delivered to Aisha Saleem at the Office of The United States Attorney 801 Cherry Street, Suite 1700, Fort Worth, TX 76102.

_____
Angela Saad